Intrusion Detection for Cyber–Physical Systems Using Generative Adversarial Networks in Fog Environment

Year: 2020 | Citations: 116 | Authors: Paulo Freitas de Araujo-Filho, Georges Kaddoum, Divanilson R. Campelo, Aline Gondim

Abstract

Cyber-attacks cyber–physical systems (CPSs) can lead to sensing and actuation misbehavior, severe damages to physical objects, and safety risks. Machine learning algorithms have been proposed for hindering cyber-attacks on CPSs, but the absence of labeled data from novel attacks makes their detection quite challenging. In this context, generative adversarial networks (GANs) are a promising unsupervised approach to detect cyber-attacks by implicitly modeling the system. However, the detection of cyber-attacks on CPSs has strict latency requirements, since the attacks need to be stopped before the system is compromised. In this article, we propose FID-GAN, a novel fog-based, unsupervised intrusion detection system (IDS) for CPSs using GANs. The IDS is proposed for a fog architecture, which brings computation resources closer to the end nodes and thus contributes to meeting low-latency requirements. In order to achieve higher detection rates, the proposed architecture computes a reconstruction loss based on the reconstruction of data samples mapped to the latent space. Other works that follow a similar approach struggle with the time required to compute the reconstruction loss, which renders them impractical for latency constrained applications. We address this problem by training an encoder that accelerates the reconstruction loss computation. Experiments show that the proposed solution achieves higher detection rates and is at least 5.5 times faster than a baseline approach in the three studied data sets.